UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

UNITED STATES OF AMERICA,	)	
	)	
v.	)	Case No. 2:20-cr-00040
	)	
TAYLOR RUFFIN HERRINGTON,	)	
	)	
Defendant.	)	

OPINION AND ORDER
DENYING DEFENDANT'S MOTION TO SUPPRESS EVIDENCE
(Doc. 57)

Defendant Taylor Ruffin Herrington (also known as "Tee") moves to suppress evidence obtained as a result of a subpoena for his Apple internet protocol (IP) address data. (Doc. 57.) The government opposes Defendant's motion. The court took this motion under advisement on July 8, 2021.

Defendant was indicted in a two count Indictment of Count I: knowingly carrying and using a firearm in relation to a drug trafficking crime in violation of 18 U.S.C. § 924(c)(1)(A), and Count II: knowingly and willfully conspiring with others to distribute heroin, a schedule 1 controlled substance, in violation of 21 U.S.C. §§ 841(a)(1), 841(b)(1)(C), 846.

The government is represented by Assistant United States Attorneys Spencer Willig and Wendy L. Fuller. Defendant is represented by Assistant Federal Public Defender Michael L. Desautels.

I. Findings of Fact.

On March 3, 2020, at approximately 2:50 a.m. Michael Haines and Amy Pudvah contacted Vermont State Police ("VSP") and reported that a person had attempted to enter their home in Cambridge, Vermont. They identified the person as "Tee" and said that he was with another individual who they identified as "Sam Simms." They reported that Tee and Sam Simms had left in Sam Simms's truck but then returned a short time later. While Mr. Haines was on the phone with VSP, he stated that he had been shot. VSP

officers arrived at Mr. Haines's and Ms. Pudvah's residence at approximately 3:50 a.m. and saw a man, later identified as Mr. Haines, on the kitchen floor. Mr. Haines was pronounced dead at 3:57 a.m. His death was declared a homicide and Defendant became the primary suspect early in the investigation. That same day, law enforcement interviewed Ms. Pudvah about the events preceding the shooting. She reported that, on March 2, 2020, Mr. Haines asked Ms. Pudvah to provide a ride for his friend Tee from Burlington to their home. When she picked Tee up in Burlington, he placed a duffel bag in the trunk of the car before getting in it. He told her that he was from Philadelphia, Pennsylvania and was born in August 1991.

When they reached Mr. Haines's and Ms. Pudvah's residence, Tee and Mr. Haines went into the basement. At approximately 8:00 p.m., they left and told Ms. Pudvah they were going to the store for beer. They returned forty minutes later and left the house again between 10:30 p.m. and 11:00 p.m. Mr. Haines returned home alone at 1:15 a.m. Ms. Pudvah asked where Tee was and Mr. Haines reported that he had dropped him off at Becky Bessette's home. Ms. Pudvah noticed that Tee's duffel bag was still in their basement. Mr. Haines left again for approximately thirty minutes and told Ms. Pudvah that he went to his friend Matthew Gillespie's house.

Ms. Pudvah was in her kitchen when she saw a dark colored pickup truck pull into the driveway. Mr. Haines told her that the car belonged to Sam Simms, instructed her to call the police, and stated that he was in a fight with Tee. Someone began to knock on the door and said that he wanted his duffel bag. Mr. Haines went into the basement, got the duffel bag, and threw it over the back deck. The pickup truck left the residence and made a right turn out of the driveway down a dead end street. Approximately fifteen minutes later, the pickup truck returned and Ms. Pudvah saw Tee at the door. Mr. Haines went to the door and told Tee that the duffel bag was out back. Ms. Pudvah saw what she thought was a pellet gun and saw Mr. Haines on the floor. Mr. Haines said that he had been shot. Ms. Pudvah showed law enforcement officers text messages on the phone that she shared with Mr. Haines and provided a phone number, 802-495-1040, which she reported belonged to Tee.

VSP officers also interviewed Ms. Bessette who told officers that Tee was using the phone number 802-234-3454, and had called her three times from that number. Ms. Bessette consented to a search of her phone which confirmed this information.

An open-source database search for the 802-495-1040 number revealed that it was connected to Verizon Wireless. A search warrant was sought for information from Verizon Wireless associated with the cellular device connected to 802-495-1040. An open-source database search for 802-234-3453 revealed that it was assigned to the carrier Bandwidth, Inc. Further investigation indicated that Bandwidth, Inc. had leased the number to Pinger, Inc. A search warrant was served on Pinger, Inc. for records related to the phone number 802-234-3453. These records revealed that the account was created on March 3, 2020, and the third-party email address provided by the user was taylor_herrington26@icloud.com and the username was taylor_herrington26. Thereafter, a grand jury subpoena was served on Apple on March 5, 2020, seeking information related to the Apple account associated with taylor_herrington26@icloud.com. The subpoena sought all customer and subscriber information for the email address and/or any related accounts that fell into the following categories: names, addresses, email addresses, telephone numbers, and usernames; records of session times and durations; length of service, types of services utilized, and devices associated with the subscriber's account; telephone or instrument number or other subscriber numbers or identity for any devices associated with the account; means and source of payment for services, including credit card or bank account number; and Apple IP logs for any device associated with the account.

From the production by Apple in response to the subpoena, law enforcement learned that the account was registered to Taylor Ruffin of 1304 W. Chelten Avenue, Philadelphia, Pennsylvania; created on November 29, 2017 and was still active; the phone number associated with the account was 215-900-3590; and the most recent iTunes update used the phone number 215-858-7026. In addition, Apple provided four spreadsheets with "account and activity information" for the taylor_herrington26 account. (Doc. 57 at 2.)

The first spreadsheet titled "iCloud Logs," contained a time-stamped log of instances in which the taylor_herrington26 account accessed various iCloud services and the IP address from which the services were accessed. *Id.* The spreadsheet included records for approximately thirteen months, from February 11, 2019 until March 5, 2020, and contained 12,880 entries. The second spreadsheet contained basic account details and the third, titled "iTunes data," included a series of sheets with time-stamped entries for the subscriber's iTunes updates. *Id.* Another spreadsheet for "iTunes Updates" contained approximately 1,174 entries. *Id.* These entries were time-stamped and included an IP address and the associated global unique identifier. The entries covered the period from March 2019 until March 2020. A spreadsheet of "iTunes Transactions" covered a similar time frame and included sixty-five time-stamped entries, an IP address, as well as a global unique identifier. *Id.* at 3. The "iDMS Signons" spreadsheet included 4,900 entries from March 9, 2019 until January 22, 2020 and documented the Apple service accessed and provided an IP address for the activity. (Doc. 57 at 3.) The final spreadsheet, "My Apple ID and iForgot data," provided approximately 160 time-stamped entries over a one year period and included the IP address from which the services were accessed. *Id.*

Law enforcement conducted an open-source database search for the phone number 215-900-3590 and determined it was assigned to AT&T. A search warrant for information related to that phone number was served on AT&T on March 9, 2020. A PEN trap was authorized to monitor that phone number. On March 9, 2020, the Federal Bureau of Investigations ("FBI") received information from AT&T that the device was in or about Philadelphia, Pennsylvania. The FBI also reviewed historical records from AT&T regarding the number 215-900-3590 and mapped cellular tower and sector information for the device which, on March 2, 2020, connected to cellular towers in Burlington, Vermont and Lamoille County, Vermont. In the early morning hours of March 3, 2020, the device connected to towers in Burlington and to towers between Burlington and Cambridge, Vermont. The device remained in Vermont until approximately March 4, 2020 when it was used to call a local taxi company before

travelling south to White River Junction, Vermont. The device continued to connect to cellular telephone towers suggesting travel to New York City and then Philadelphia.

On March 12, 2020, a grand jury subpoena was served on the carrier associated with 267-250-0072.[1] The records received pursuant to the subpoena indicated that the subscriber was Taylor Ruffin and the phone number associated with the account from April until June 2019 was 267-624-3449. That same day, Defendant was indicted for violations of 18 U.S.C. § 924(c)(1)(A) and 21 U.S.C. §§ 841(a)(1)(C), 841(b)(1)(C), 846 and a warrant was issued for his arrest. Law enforcement subsequently arrested Defendant at his apartment.

On March 13, 2020, Google was served with a grand jury subpoena requesting subscriber information for any Google accounts associated with 802-495-1040, 215-900-3590, and/or the device identifiers associated with those numbers. Google responded that the Google account jr5555976@gmail.com was associated with 802-495-1040. It was determined that the account was created on December 29, 2019, and was last logged into on February 14, 2020. The sign-in phone number and recovery SMS phone number was 802-495-1040.

On August 20, 2020, FBI Task Force Officer Jeffrey Stephenson applied for a warrant to search the contents of the Apple iCloud account taylor_herrington26@icloud.com. Officer Stephenson provided an affidavit in which he summarized the type of data typically contained in an iCloud account, noting that: "IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation." (Doc. 22-3 at 17, ¶ 40.) Officer Stephenson described the process by which an IP address can produce further information: "[u]sing www.ip2location.com, which is an open source Internet search site which I have found to be reliable in the past, I learned that 107.77.223.78 is an AT&T Mobility IP address. At

[1] There is no information regarding how law enforcement discovered this number or determined that it was associated with Defendant.

least three of the additional IP addresses provided in the IP logs also resolved back to AT&T Mobility according to www.ip2location.com." *Id.* at 9, ¶ 19. The records produced contained the same information as those from the subpoena of the same Apple iCloud account issued on March 5, 2020.

On September 3, 2020, a search warrant was issued permitting law enforcement to search information associated with jr5555976@gmail.com. The search warrant application noted that law enforcement discovered this email address through information from a subpoena of Google records associated with 802-495-1040.

A subpoena was served on Google on October 1, 2020, requesting records related to jayruffin89@gmail.com. Those records revealed that the name associated with the account was Taylor Ruffin-Herrington with a recovery SMS number of 267-624-3449. The recovery email for the account was ruffin_taylor@yahoo.com.

On October 29, 2020, a search warrant was obtained for information associated with the email account: jaye.ruffin89@gmail.com. The warrant application noted that law enforcement discovered this email address after receiving the search warrant return from the Apple iCloud account taylor_herrington26@icloud.com. Within those files, there was screen shot image in the iCloud photo library which revealed an address/Google account jaye.ruffin@gmail.com and a phone number of 267-624-3449.

II. Conclusions of Law and Analysis.

A. Whether Defendant had a Reasonable Expectation of Privacy in his IP Address Logs.

Defendant contends that he had a reasonable expectation of privacy in the subpoenaed IP addresses because that information can be used to identify his historical geographic locations. He challenges the government's subpoena and the August 20, 2020, search warrant that allegedly enabled law enforcement to determine his location. He points out that the August 20, 2020 warrant application itself notes that "every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account[]" and that

this information "allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation." (Doc. 22-3 at 17, ¶ 40.) He argues that the government improperly used subpoenas to obtain location information.

The government counters that information sought in this case differs from warrantless access to historical cell-site location information ("CSLI") which reveals "detailed" and "encyclopedic" location information that is "effortlessly compiled" without any volitional act by the customer because it is collected whenever a phone is turned on and connected to a network. (Doc. 62 at 4) (quoting *Carpenter v. United States*, 138 S. Ct. 2206, 2216, 2219-20 (2018)). It argues that, "IP data is distinguishable from CSLI in [two] respects: IP logs do not effortlessly or even necessarily convey location information; and IP data [is] only generated if and when a user chooses to access a particular website or application." *Id.*

The Fourth Amendment to the United States Constitution provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. AMEND. IV.

"[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). The Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *see also United States v. Miller*, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities[.]").

In *Carpenter*, the Supreme Court held that CSLI was not subject to the third-party doctrine because "the notion that an individual has a reduced expectation of privacy in

information knowingly shared with another" or that an individual has engaged in "voluntary exposure" by his or her mere physical movements through the use of a cell phone, extends the doctrine too far. 138 S. Ct. at 2219-20. As a result, "[w]hether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier, . . . an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Id.* at 2217. The Supreme Court focused on the "special solicitude for location information" which protects individuals from warrantless searches of "detailed chronicle[s]" of their movements. *Id.* at 2219-20. It described its holding as "narrow" and stated that it "[did] not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor [does it] address other business records that might incidentally reveal location information." *Id.* at 2220.

As the Eleventh Circuit has observed "every circuit to consider the question after *Carpenter*" has held that IP address logs are subject to the third-party doctrine as "business records" and have distinguished between an IP address and CSLI. *United States v. Trader*, 981 F.3d 961, 968, 969 (11th Cir. 2020) (denying a defendant's motion to suppress because IP address data does not "directly record[] an individual's location. An [IP] address is a string of characters associated in an internet provider's business records with a particular device connecting to the internet through a particular network. Internet protocol addresses can be translated into location information only indirectly, by examining the internet company's business records to determine the physical address where the network is registered.") (internal citation omitted); *see also United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018) (concluding that IP address data "comfortably within the scope of the third-party doctrine[]" because the third party's "records revealed only that the IP address was associated with the [defendant's] residence[]" and "had no bearing on any person's day-to-day movement"); *United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019) (holding that "an internet user generates the IP address data that the government acquired from [a phone application] only by making the affirmative decision to access a website or application[]" whereas "every time a cell

phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell site tower without the cell phone user lifting a finger"); *United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. 2019), *cert. denied*, 140 S. Ct. 876 (2020) (finding that the defendant "had no reasonable expectation of privacy in his IP address or subscriber information"); *United States v. VanDyck*, 776 F. App'x 495, 496 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 295 (2020) (finding that the defendant had "no expectation of privacy in the IP addresses of the websites [he] visit[ed]") (citing *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)).

Defendant nonetheless argues that an IP address is akin to CSLI because "the information obtained in this case amounted to thousands of records that covered many months" and "the records produced . . . are produced constantly, whenever a device is used. . . . For example, the 11,000 entries that were part of the iCloud IP address log produced by Apple were compiled at the rate of several hundred per day[] . . . [and] the Apple records applied not just to one device, but appear to have been produced anytime an Apple device or service were used by the account holder." (Doc. 57 at 8-9.) He asserts that "the records in this case were also retrospective" and "give the authorities access to retrospective data that provide physical as well as digital location information." *Id.* at 9. He contends that "the authorities received tens of thousands of time-stamped IP address entries. Such a detailed IP log would tend to reveal a picture of where the customer used the services over time. . . . the government can use this type of information to tie an individual to a digital or physical location." *Id.* at 11.

Although Defendant analogizes an IP address to CSLI by asserting that some geographic location information may be gleaned from an IP address, he cites no authority for the proposition that the ability to use an IP address for other investigative purposes creates an expectation of privacy that does not otherwise exist. The Supreme Court's "narrow" holding in *Carpenter* did not "disturb the application of *Smith* and *Miller*" or "address other business records that might incidentally reveal location information." *Carpenter*, 138 S. Ct. at 2210. As the *Trader* court held, IP addresses "are neither location records nor cell phone records[]" and "can be translated into location

information only indirectly[.]" *Trader*, 981 F.3d at 968 (citing *Hood*, 920 F.3d at 92). "[U]nlike CSLI, 'an internet user generates the IP address data . . . only by making the affirmative decision to access a website or application.'" *United States v. Morel*, 922 F.3d 1, 9 (1st Cir. 2019) (quoting *Hood*, 920 F.3d at 92-93). No federal Circuit Court of Appeals has recognized a reasonable expectation of privacy in an IP address.[2]

Because Defendant has not established a reasonable expectation of privacy in his IP address logs, his motion to suppress must be DENIED. *See United States v. Delva*, 858 F.3d 135, 148 (2d Cir. 2017); *see also United States v. Sparks*, 287 F. App'x 918, 919 (2d Cir. 2008) (holding that a defendant "bears the burden of showing that he had a reasonable expectation of privacy" in the area or item searched) (citing *California v. Greenwood*, 486 U.S. 35, 39 (1988)).

B. Whether the Good Faith Exception Should Apply.

The government contends that the good faith exception should apply to its use of subpoenas to access IP logs because it "extend[s] . . . to searches conducted in reasonable reliance on subsequently invalidated statutes." *Davis v. United States*, 564 U.S. 229, 239 (2011) (citing *Illinois v. Krull*, 480 U.S. 340 (1987)). Defendant asserts that law

---

[2] *See United States v. Ulbricht*, 858 F.3d 71, 97 (2d Cir. 2017), *abrogated on other grounds by United States v. Chambers*, 752 F. App'x 44, 47 (2d Cir. 2018) ("The recording of IP address information and similar routing data, which reveal the existence of connections between communications devices without disclosing the content of the communications, are precisely analogous to the capture of telephone numbers at issue in *Smith*."); *United States v. Caira*, 833 F.3d 803, 806-09 (7th Cir. 2016) ("Because [the defendant] voluntarily shared his I.P. addresses with Microsoft, he had no reasonable expectation of privacy in those addresses."); *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) ("[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs."); *United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008) ("[E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."); *United States v. Hammalian*, 2018 WL 1951201, at *4 (D. Vt. Apr. 24, 2018) (denying the defendant's motion to suppress internet subscriber information and holding that "[t]he third-party disclosure doctrine is . . . 'dispositive' to the extent that [the d]efendant 'cannot claim a reasonable expectation of privacy in the government's acquisition of his subscriber information, including his IP address and name from third-party providers'") (quoting *United States v. Wheelock*, 772 F.3d 825, 828-29 (8th Cir. 2014)).

enforcement did not rely on a statute or law to subpoena the IP address logs, however, the government cites 18 U.S.C. § 2703(c)(2)(E) as support for its subpoenas. 18 U.S.C. § 2703(c)(2) states:

> A provider of electronic communication service or remote computing service shall disclose to a governmental entity the . . . telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address . . . of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or by any means available under paragraph (1).

This statute grants law enforcement the authority to use subpoenas to access IP address logs.

Here, there is no ground to find law enforcement's reliance on 18 U.S.C. § 2703(c)(2)(E) unreasonable because "in passing the statute, the legislature [did not] wholly abandon[] its responsibility to enact constitutional laws[]" and "its provisions are [not] such that a reasonable officer should have known that the statute was unconstitutional." *Krull*, 480 U.S. at 355. Following *Carpenter*, courts continue to hold that IP address data may be subpoenaed without violating the Fourth Amendment.

Because law enforcement's reliance on 18 U.S.C. § 2703(c)(2)(E) was objectively reasonable, Defendant's motion to suppress unspecified "fruit of the poisonous tree" evidence obtained pursuant to a subpoena is also DENIED.

CONCLUSION

For the reasons stated above, Defendant's motion to suppress evidence is DENIED. (Doc. 57.)

SO ORDERED.

Dated at Burlington, in the District of Vermont, this 9th day of August, 2021.

Christina Reiss, District Judge
United States District Court